USDA UNITED STATES DEPARTMENT OF AGRICULTURE

Windows 2000 Server

Security Assessment Guide

July 9, 2001

Prepared by:
Barre Bull, Sr. IT Security Analyst
Don Truax, HW/SW Installation Tech

SAIC Science Applications International Corporation
An Employee-Owned Company
1953 Gallows Rd., 2nd Floor
Vienna, VA 22182

SAIC-6099-2001-224

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

For Official Use Only

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Microsoft Windows 2000 Server Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Microsoft Windows 2000 Server. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data. This checklist does not address applications installed on the system or special purpose configurations (i.e. web servers, database servers, etc.).

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, and "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements. USDA does not currently have a comprehensive security risk assessment process. This guide is intended to serve as an interim measure, until formal risk assessment policies and procedures can be developed and implemented.

4. REFERENCES

a. External

(1) Public Law 100-235, "Computer Security Act of 1987"
(2) Public Law 93-579, "Privacy Act of 1974"
(3) Public Law 93-502, "Freedom of Information Act"
(4) Public Law 99-474, "Computer Fraud and Abuse Act"
(5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.

(6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

(1) DR 3140-001, "USDA Information Systems Security Policy" dated may 15, 1996

(2) DM 3140-1 "USDA Management ADP Security Manual" dated March 5, 1992

Windows 2000 Server Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met or mitigated, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency/System Identification:

Agency/System	
Address	
Date of last Assessment:	

Test Number: **1**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Microsoft Windows 2000 Server Access and Configuration			
Resources Required:	Access to the Microsoft Windows 2000 Server Primary Domain Controller server, Administrative ID and Password for server.		
Personnel Required:	Microsoft Windows 2000 Server Systems Administrator.		
Objectives:	To determine that the Microsoft Windows 2000 Servers are configured to meet USDA requirements pertaining to systems protection, user access privileges and virus protection. To determine that file servers are not being used as workstations and that they are located in restricted areas.		
Procedure Description: (Summary)	Verify that access is properly controlled; virus protection software is installed, configured and functioning properly. Verify that file servers are not being used as workstations and that they are located in restricted areas. Verify version and service pack level of operating system.		

Detailed Procedures and Results

Step #	**Procedure Description**	**Expected Results**	**Actual Results** **(if different from Expected)**	**Y/N/P**
1.	Observe that the system to be assessed is locked or that a password-protected screensaver has been implemented.	System is locked or a password-protected screensaver is active.		
2.	Ask the System Administrator if the CMOS on all servers are password protected.	The CMOS on all servers are password protected.		
3.	Ask the System Administrator if the server CMOS has been configured to boot only from the hard drive.	The server CMOS has been configured to boot only from the hard drive.		
4.	Ask the System Administrator if the hard drive is formatted using NTFS.	Hard drive is formatted using NTFS.		
5.	Ask the System Administrator if there is an up-to-date Emergency Repair Disk for the system.	There is an up-to-date Emergency Repair Disk for the system.		
6.	Ask the System Administrator if the Emergency Repair Disk is stored in a secure environment.	The Emergency Repair Disk is stored in a secure environment.		

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
7.	Use the Secure Attention Sequence (Ctrl+Alt+Delete) to access the server logon screen.	Logon screen appears.		
8.	Verify that a Legal Notice dialog box appears prior to the Logon dialog box.	A Legal Notice dialog box appears prior to the Logon dialog box.		
9.	Click the OK button in the Legal Notice dialog and continue with log on.	Logon Dialog window is presented on screen.		
10.	Verify that there is no User ID from a previous session in the User ID portion of the logon window.	There is no User ID from a previous session in the User ID portion of the logon window.		
11.	Observe how many buttons are available on the logon window. .	3 buttons are available on the logon window, the Logon, Options, and Cancel button. Shutdown is grayed out.		
12.	Ask the SA if the Guest account has a password.	Guest account has a password.		
13.	Attempt to logon to the system using the User ID Guest and pressing return (do not enter a password).	Access denied.		
14.	Attempt to logon to the system using the User ID Guest and enter Guest for the password.	Access denied.		
15.	Attempt to logon to the system using the User ID Administrator and pressing return (do not enter a password).	Access denied.		
16.	Attempt to (or have system administrator) logon to the system using a valid non-administrator User ID and password.	Logon in Process message window appears.		
17.	Ask the System Administrator if local or centralized virus scanning is used.	If local virus scanning is used skip to question 18.		
18.	If centralized virus scanning is used ask the System Administrator if the virus signatures are kept current on the central scanning system.	Most current version of the virus signatures is being used. Skip to question 21		
19.	When the desktop appears observe the system tray in the bottom right corner of the desktop to verify that a virus protection software icon is	Virus protection software icon is present.		

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
	present.			
20.	Have SA show the date of the virus patterns/signatures currently running.	The patterns/signatures should be no more than one month old.		
21.	Open Start menu, select Programs and observe the programs listed.	There are no programs listed that are not necessary to the functioning of the server.		
22.	Ask the SA if shared system and security software files are protected from unauthorized access and modification.	Shared system and security software files are protected from unauthorized access and modification.		
23.	Open Start menu and click on Settings.	Settings menu appears.		
24.	Click on Control Panel	Control Panel window opens.		
25.	Right click the System Icon and select Properties.	Display Properties menu opens.		
26.	Select the General Tab and verify that the Operating System is Microsoft Windows 2000.	The operating system is Microsoft Windows 2000.		
27.	Verify that the current Service Pack is installed.	The current Service Pack has been installed.		
28.	Exit the System Properties Menu.	System Properties windows close.		
29.	Click on the Start menu button in the task bar.	Start menu opens.		
30.	Click on the Programs selection.	Program menu appears.		
31.	Select Administrative Tools.	Administrative Tools menu appears.		
32.	Select Computer Management | Local Users and Groups| Users.	Computer Management | Local Users and Groups | Users window opens.		
33.	Observe that the Administrator account has been renamed.	Administrator account has been renamed.		
34.	Ask the SA if the Administrator account is used.	Administrator account is not used.		
35.	Ask the SA if users requiring administrative access to servers have individual accounts with membership in the Administrators Group.	Users requiring administrative access to servers have individual accounts with membership in the Administrators Group.		

36.	Right click on the Guest icon, open Guest Properties and observe that the User Cannot Change Password, Password Never Expires and Account is Disabled boxes are checked.	User Cannot Change Password, Password Never Expires and Account is Disabled boxes are checked.		
37.	Click on the Member Of button in the Guest account properties window and observe what the Guest account is a member of.	Guest account is a member of no User Group.		
38.	Click the OK button and close Guest account properties window.	Guest account properties dialog window closes.		
39.	Ask SA if system rights/permissions are assigned based on Group membership of users.	Rights/permissions are assigned based on Group membership of users.		
40.	Ask SA if rights/permissions are assigned to domain groups or individual users.	Rights/permissions are assigned to domain group’s not individual users.		
41.	Ask SA if users are assigned to groups based on job function and/or “need to know.”	Users are assigned to groups based on job function and/or “need to know.”		
42.	Observe Groups listing in the Groups Folder to ensure that only Approved Groups exist.	Only Approved Groups exist.		
43.	Exit the Computer Management Menu.	Computer Management Menu closes.		
44.	Ask the SA if the servers are used as workstations and observe that physical access is restricted.	Servers are not used as workstations and physical access to the file servers is restricted.		
45.	Ask SA if unnecessary services have been disabled.	Unnecessary services have been disabled. (Services will be different from system to system in some cases and generally be determined locally.)		

Comments:

Action Plan:

Test Number: **2**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Microsoft Windows 2000 Domain Controller Password Policy Configuration			
Resources Required:	Access to the Domain Controller with Administrator Access		
Personnel Required:	Microsoft Windows 2000 Server Systems Administrator.		
Objectives:	To determine that the Microsoft Windows 2000 Server Password Policies are configured to meet USDA requirements pertaining to Identification and Authentication.		
Procedure Description: (Summary)	Verify that Password Policies are properly configured.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Select Start |Programs | Administrative Tools |Local Security Policy | Account Policy's |Password Policy |Minimum Password Policy | Ensure Local Policy Settings is set to 8.	Local Password Policy Setting is set to 8 characters. Note: a 0 setting will allow a blank password.		
2.	Click on Start Menu button |Programs | Administrator Tools| Local Security Policy	The Security Policy MMC appears.		
3.	Click on the Account Policies Menu button of the Local Security Settings window.	Account Policy menu screen appears on the right side.		
4.	Verify that the account policies match those on the Microsoft Windows 2000 Server Account Policy settings attachment. (See Attachment 3A and 3B)	The account policies match those on the Microsoft Windows 2000 Server Account Policy Settings attachment.		
5.	Select Password Policy on left side of window	Password Policy setting open in right window		
6.	Enforce password history is set to 5 passwords remembered	Local Setting = 5 passwords remembered Effective Setting = 5 passwords remembered		
7.	Maximum password age is set to 90 days	Local Setting = 90 days Effective Setting = 90 days		
8.	Minimum password age is set to 7 days	Local Setting = 7 days Effective Setting = 7 days		
9.	Minimum password length is	Local Setting = 8		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	set to 8 characters	characters Effective Setting = 8 characters		
10.	Passwords must meet complexity requirements	Local Setting =Enabled Effective Setting = Enabled		
11.	Store password using reversible encryption for all users in the domain	Local Setting =Enabled Effective Setting = Enabled		
12.	Click on Account Lockout Policy in left window	Account Lockout policy appears in right window		
13.	Lock out duration is set to 0 to enable lockout Forever – Until unlocked by Administrator	Local Setting = 0 Effective Setting = 0		
14.	Lock Out is set to lock out after 3 failed login attempts	Local Setting = 3 Effective Setting = 3		
15.	Lock out is set to reset count after 60 minutes	Local Setting = 60 Effective Setting = 60		
16.	Click OK.	Account settings screen closes.		

Comments:

Action Plan:

Test Number: **3**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Microsoft Windows 2000 Server Registry Settings			
Resources Required:	Administrative access to the Microsoft 2000 Server Domain Controller.		
Personnel Required:	Microsoft Windows 2000 Server System Administrator.		
Objectives:	To verify that all registry settings in place and correct.		
Procedure Description: (Summary)	Using Regedt32 to access the system registry and verify that specific registry keys are correctly configured. **WARNING: This test must be done carefully to prevent any damage to the registry. DO NOT ATTEMPT TO EDIT THE REGISTRY!**		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
1.	Click on the Start button in the Task Bar.	Start menu choices appear.		
2.	Click on Run.	Run Dialog window opens.		
3.	Enter Regedt32 in the Run dialog.	Regedit starts and the Registry tree appears in the left window.		
4.	Select the HKEY_LOCAL_MACHINE folder.	Hive categories appear.		
5.	Click on Security at the top and select Permissions	Registry Permissions dialog window opens		
6.	Ensure Permissions are correct.	Administrators-Full Control Everybody-Read Only System-Full Control		
7.	Select the Advance button in the Security interface and ensure that in the Permissions interface the check box for Reset Permissions on all child objects and enable propagation of inheritable is “NOT CHECKED”	The check box for Reset Permissions on all child objects and enable propagation of inheritable is “NOT CHECKED”		
8.	While in the Permissions interface select the Advance Button | Auditing Tab | Add Button | and select Everyone. Ensure that all Success and Fail checkboxes are selected. Ensure that the “Allow inheritable auditing entries from parent to propagate to this object is not checked.	Everyone is selected with all Success and Fail checkboxes selected. Stated checkbox is selected.		
9.	Exit Permissions dialog window	Permissions dialog window closes		
10.	Select Software.	Software categories		

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
		appear.		
11.	Select Microsoft.	Microsoft categories appear.		
12.	Select Windows NT	Windows NT categories appear.		
13.	Select Current Version.	Current Version categories appear.		
14.	Select Winlogon	Winlogon edit string appears.		
15.	Observe the LegalNoticeCaption in the right side of the window and verify that the text string is “AUTHORIZED USE ONLY.”	The text string within the double quotes is “AUTHORIZED USE ONLY.”		
16.	Observe the LegalNoticeText in the right side of the window and verify that it is equivalent to the text in Attachment 1.	The text within the double quotes matches or is equivalent to the text in the Attachment 1.		
17.	Observe the DontDisplayLastUserName entry in the right window and verify that a “1” appears in the double quotes.	A “1” appears in the double quotes.		
18.	Verify that the ShutdownWithoutLogon value is set to 0.	ShutdownWithoutLogon value is set to 0.		
19.	Select \Program Groups\ Select the "Security" tab at the upper middle of the interface, then "Permissions" from the menu Then select Advance\Auditing Tab\Add Tab and double click “Everyone” and verify that all Successful and Failed check boxes are checked.	All Successful and Failed check boxes are checked showing all significant changes are audited.		
20.	Select \Microsoft\OS/2 and ensure that the \OS/2 Subsystem for NT contains no subkeys.	\MicrosoftOS/2 Subsystem for NT contains no subkeys. **Note:** These subsystems were not included in the evaluated configuration, and therefore C2-like compliance cannot be achieved unless they are removed.		
21.	Select HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\LSA. The	RestrictAnonymous has been created and the value is 1.		

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
	RestrictAnonymous should be present and the value should be set to 1.	**Note**: This setting restricts anonymous users from being able to obtain public information about the LSA component of the Windows NT Security Subsystem. The LSA handles aspects of security administration on the local computer, including access and permissions.		
22.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems and verify there are no entries for Posix and OS/2	There are no entries for Posix and OS/2. **Note:** These subsystems were not included in the evaluated configuration, and therefore C2-like compliance cannot be achieved unless they are removed.		
23.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ ProtectionMode and verify that the value is set to 1.	ProtectionMode value is set to 1. **Note:** This step is necessary to further heighten security of the base objects. Among other things, it prevents users from gaining local administrator privileges by way of a dynamic-link library (DLL).		
24.	Select HKEY_LOCAL_MACHINE\SYSTEM\Optional and verify that there are no values listed.	HKEY_LOCAL_MACHINE\SYSTEM\Optional does not exist or No values are listed are listed.		
25.	Double click on the "HKEY_CLASSES_ROOT". Select the "Security" tab at the upper middle of the interface, then "Permissions" from the menu.	Verify that permissions on “HKEY_CLASSES_ROOT" and all its subkeys are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read System - Full Control		

Step #	Procedure Description	Expected Results	Actual Results (if different from Expected)	Y/N/P
		NOTE: The box "Allow inheritable permissions from parent to propagate to this object" is NOT checked. [Default]		
26.	Select "HKEY_USERS" \ .DEFAULT \UNICODE Program Groups\". Select the "Security" tab at the upper middle of the interface, then "Permissions" from the menu.	Verify that permissions on "HKEY_USERS\.DEFAULT \UNICODE Program Groups\[all subkeys]" are set to: Administrators - Full Control Everyone - Read System - Full Control		
27.	Exit Regedt32			

Comments:
Action Plan:

Test Number: **4**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Microsoft Windows 2000 Server Audit			
Resources Required:	Access to the Microsoft Windows 2000 Domain Controller or server with Administrator Access		
Personnel Required:	Microsoft Windows 2000 Systems Administrator.		
Objectives:	To determine that the Windows 2000 servers are configured to meet USDA requirements pertaining to Auditing.		
Procedure Description: (Summary)	Verify that auditing is turned on, functioning and properly configured. Also, verify that the audit logs are reviewed on a regular basis and backed up on a regular schedule.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Ask the SA if there is a documented schedule for the review of the Audit logs.	Audit logs are reviewed per documented schedule.		
2.	Ask the SA if the audit logs are backed up according to a routine schedule. Observe back-ups of audit logs.	Audit logs are backed up according to a routine schedule.		
3.	Ask the SA if there are procedures in place for moving the logs off the system when they become full.	There are procedures in place for moving the logs off the system when they become full.		
4.	Ask the SA if copies of the audit log backups are stored in a secure environment offsite.	Copies of the audit log backups are stored in a secure environment offsite.		
5.	Click Start | Programs | Administrative Tools | Event Viewer.	Event Viewer window opens.		
6.	Select the Application Log and select properties from the Actions menu.	Application Log Events dialogue box appears in the right side window. Application Log Properties dialogue box appears.		
7.	Select General tab and verify that.	“Do Not Overwrite” box is checked.		
8.	Click the OK button at the bottom of the Application Log Properties menu.	Application Log Properties Settings Dialogue window closes.		
9.	Select the Security Log and	Security Log Events		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	select properties from the Actions menu.	dialogue box appears in the right side window. Security log settings dialogue box appears		
10.	Select the Filter tab and check mark all options in Event types. (See attachment 4)	Unsuccessful log-on attempts are shown in the audit log.		
11.	Select General tab and verify that.	"Do Not Overwrite" box is checked.		
12.	Click the OK button at the bottom of the Security Log Properties menu.	Security Log Properties Settings Dialogue window closes.		
13.	Select the System Log and select properties from the Actions menu.	System log settings dialogue box appears in the right side window. System log settings dialogue box appears		
14.	Select General tab and verify that	"Do Not Overwrite" box is checked.		
15.	Click the OK button at the bottom of the System Log Properties menu.	System Log Properties Settings Dialogue window closes.		

Comments:

Action Plan:

Test Number: **5**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Microsoft Windows 2000 Server System Backups			
Resources Required:	Access to the Microsoft Windows 2000 Server Primary Domain Controller server (or server used for backups) with Administrator Access		
Personnel Required:	Microsoft Windows 2000 Server Systems Administrator.		
Objectives:	To ensure that Microsoft Windows 2000 Server operating systems and applications are backed up on a timely basis and that backup procedures are being performed.		
Procedure Description: (Summary)	Examine backup scheduler program and log files to determine that backups are conducted on a timely basis. Review Microsoft Windows 2000 Server backup procedures and determine that procedures are being performed. Ensure that copies of back-ups are stored off-site.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Review backup scheduler programs and log files to determine that backups are conducted on a timely basis.	Backups are conducted on a timely basis.		
2.	Ask Administrator for Server backup procedures document and ask if the procedures are being followed.	Server backup procedures documentation available and procedures are being performed as required.		
3.	Ask Administrator if Server backups are tested.	Server backups are tested.		
4.	Ask SA if copies of backups are stored off-site.	Copies of backups are stored off-site.		
5.	Ask SA if copies of backups are stored in a secure environment “off-site” on a regular basis.	Copies of backups are stored in a secure environment “off-site” on a regular basis.		

Comments:

Action Plan:

ATTACHMENT 1

Legal Notice Text string:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT…

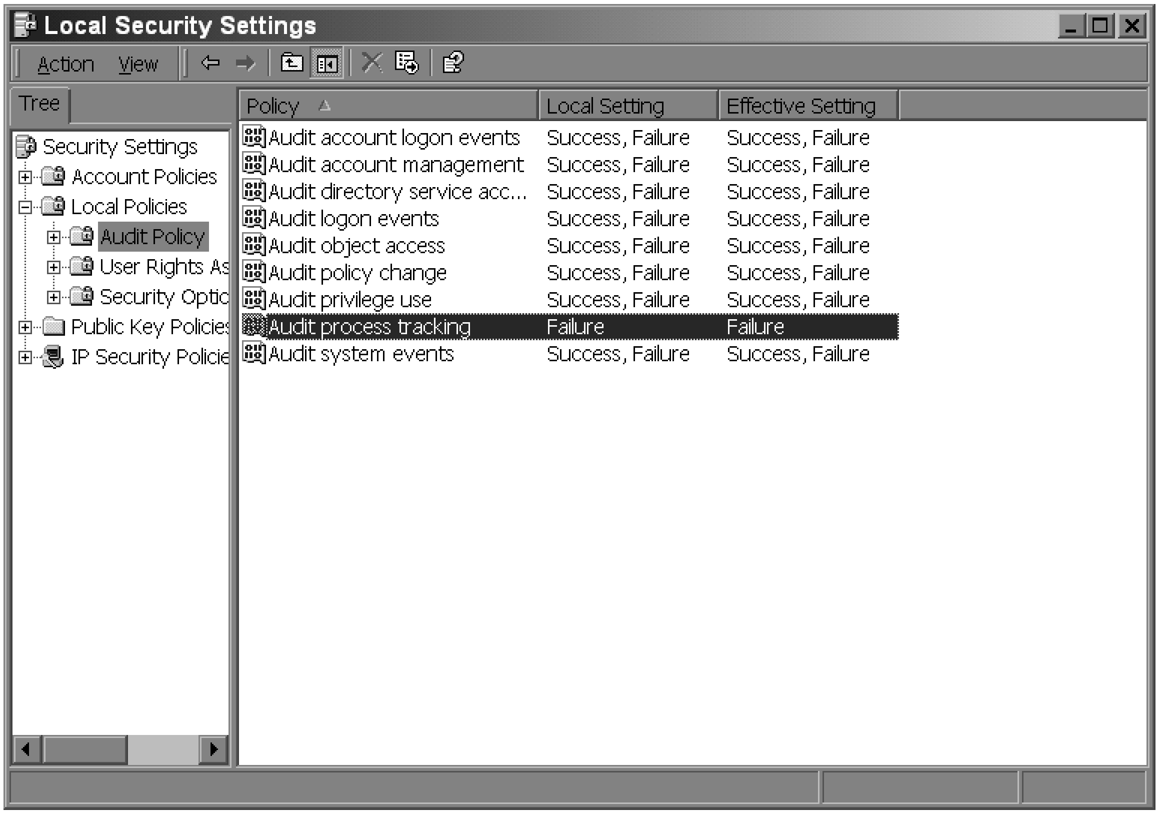
Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER

ATTACHMENT 2

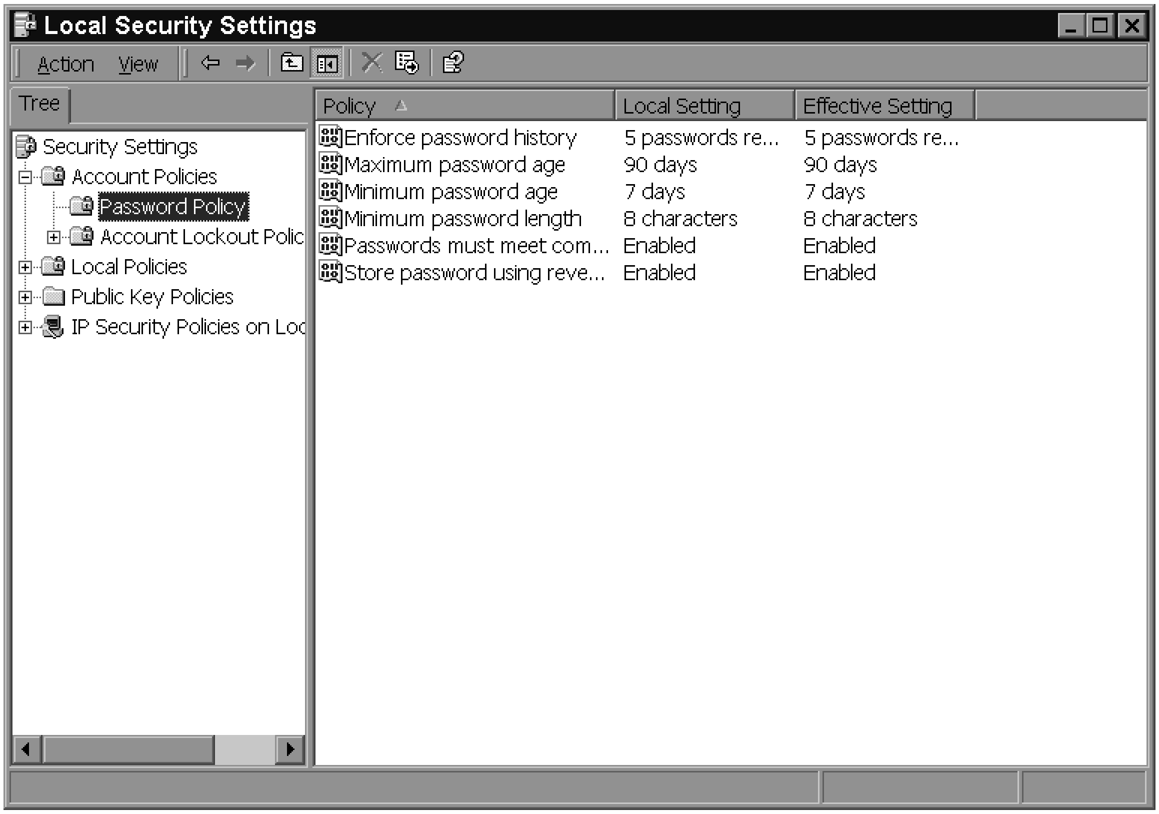
Microsoft Windows 2000 Server Audit Policy Settings:



Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service acc...	Success, Failure	Success, Failure
Audit logon events	Success, Failure	Success, Failure
Audit object access	Success, Failure	Success, Failure
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Success, Failure	Success, Failure
Audit process tracking	Failure	Failure
Audit system events	Success, Failure	Success, Failure

ATTACHMENT 3 A

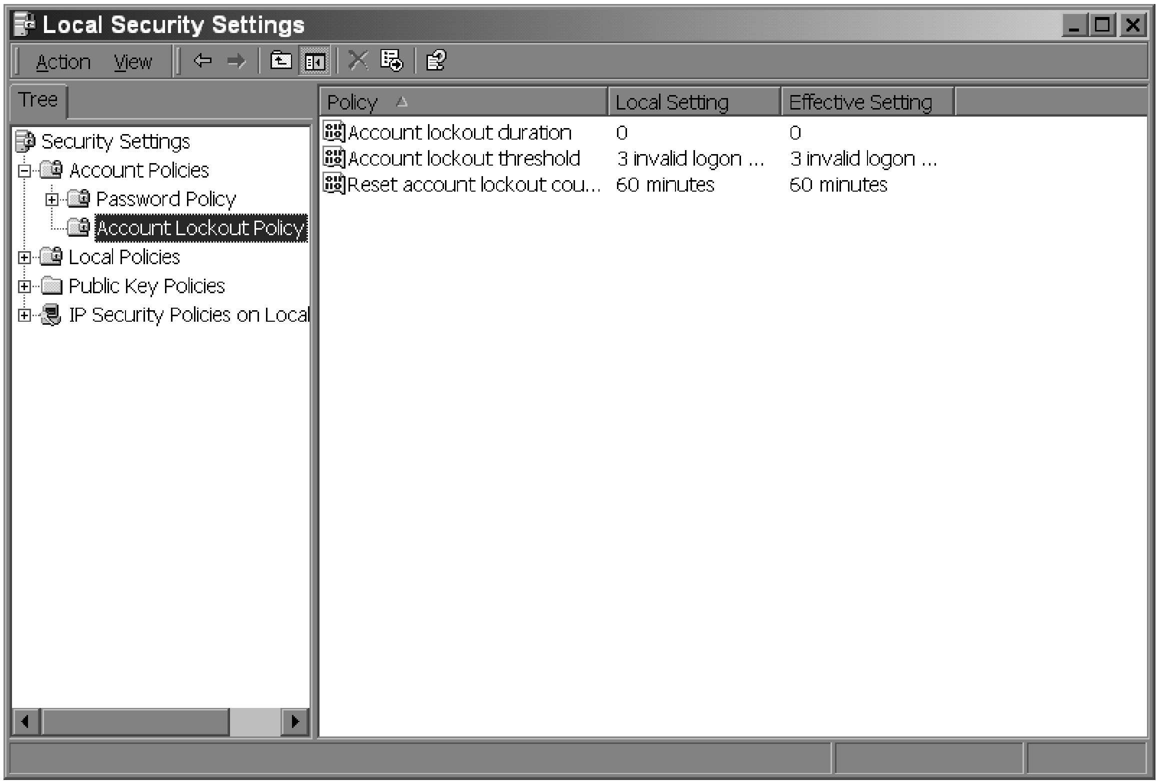
Microsoft Windows 2000 Server Password Policy Settings:



Policy	Local Setting	Effective Setting
Enforce password history	5 passwords re...	5 passwords re...
Maximum password age	90 days	90 days
Minimum password age	7 days	7 days
Minimum password length	8 characters	8 characters
Passwords must meet com...	Enabled	Enabled
Store password using reve...	Enabled	Enabled

ATTACHMENT 3 B

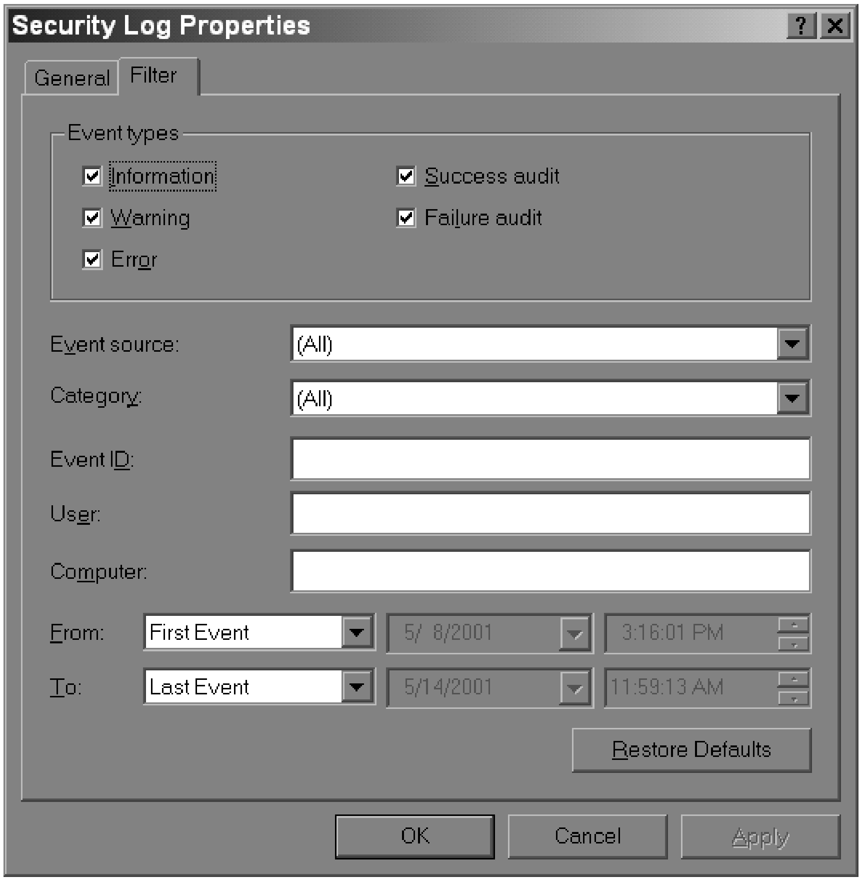
Microsoft Windows 2000 Server Account Lockout Policy Settings:



Policy	Local Setting	Effective Setting
Account lockout duration	0	0
Account lockout threshold	3 invalid logon ...	3 invalid logon ...
Reset account lockout cou...	60 minutes	60 minutes

ATTACHMENT 4

Microsoft Windows 2000 Server Security Log Properties:



☑ Information ☑ Success audit

☑ Warning ☑ Failure audit

☑ Error

Event source: (All)

Category: (All)

Event ID:

User:

Computer:

From: First Event 5/ 8/2001 3:16:01 PM

To: Last Event 5/14/2001 11:59:13 AM